Systémy odolné proti poruchám – metodika návrhu řadiče rekonfigurace

Richard Pánek
1. ročník, prezenční studium
školitel: Doc. Ing. Zdeněk Kotásek, CSc.

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 2, 612 66 Brno, Česká republika
Tel.: +420 54114-1362
Email: ipanek@fit.vutbr.cz

***Abstrakt*—Pro kritické nejen řídicí systémy je výskyt poruch velice nežádoucí záležitostí. Obzvláště pokud by mohlo dojít k újmě na zdraví nebo finančním ztrátám. Proto se rozvíjely techniky známé pod názvem systémy odolné proti poruchám. Pro zotavování z poruch je využití rekonfigurace obzvláště výhodné. Platformou schopnou rekonfigurace pro návrh a implementaci obvodů je FPGA. Pro zajištění opravy obvodu v FPGA pomocí rekonfigurace je velice výhodné využít řadič částečné dynamické rekonfigurace tedy speciální přidanou komponentu. Dále je žádoucí, aby i řadič byl odolný proti poruchám, obzvláště když bude umístěn na stejném FPGA. Právě vypracováním příslušných kritérií a návrhem tohoto řadiče se bude zabývat metodika, která bude také tématem disertační práce.**

***Klíčová slova*—Řadič rekonfigurace, systémy odolné proti poruchám, částečná dynamická rekonfigurace, FPGA.**

I. Úvod

V dnešní době nás obklopují elektronická zařízení v nejrůznějších přístrojích všeho druhu. Podle jejich určení se klade důraz na výkon, spotřebu, cenu, atd. Ovšem existují také aplikace, kde je potřeba zajistit spolehlivost. Ta je vyžadována obzvláště u systémů, kde by mohlo dojít k újmě na životech nebo na financích. Typickými zástupci takových aplikací jsou řídicí systémy, které se starají o řízení letadel, družic, elektráren, ale také třeba nemocničních přístrojů a mnoha dalších. Je zřejmé, že se jedná o systémy, které musí pracovat bezchybně anebo se musí umět z vlastních poruch zotavit, popř. i přes poruchu pracovat správně.

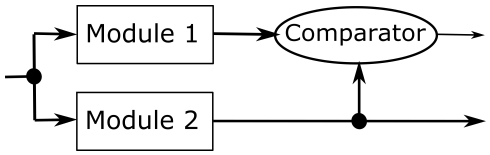
Tento článek je dále uspořádán následovně. Sekce II je zaměřena na uvedení do problematiky a objasnění pojmu *Odolnost proti poruchám*. Je zde vysvětleno možné dělení a také základní přístupy. Sekce III se věnuje řadiči částečné dynamické rekonfigurace pro FPGA. Kromě obecných možností je zaměřena na konkrétní implementaci a také na budoucí výzkum, který bude pokračovat nad touto problematikou. Obzvláště se jedná o možnosti jeho zabezpečení a tím zvýšení jeho spolehlivosti. Sekce IV pojednává o posledním nezabezpečeném prvku volícím majoritu. V sekci V jsou nastíněny cíle disertační práce. Závěrečné shrnutí je v sekci VI.

II. Odolnost proti poruchám

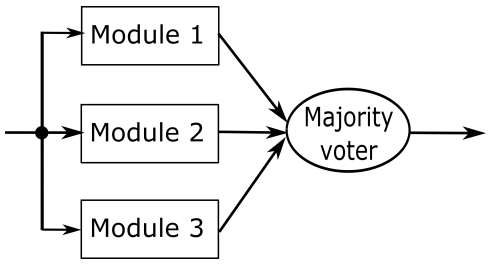
Odolnost proti poruchám (Fault tolerance) [5] je přístup, kdy je systém schopen pracovat dle specifikace i přes výskyt poruch. Snižování dopadu poruch je možné dosáhnout využitím prostorové, časové nebo datové redundance. Jejich volba záleží na požadavcích výsledné aplikace. Prostorová redundance znamená několikanásobný výskyt stejných komponent, které pracují současně. Oproti tomu časová redundance je dána prováděním stejného výpočtu několikrát na stejné komponentě. Datovou redundancí je myšleno opatření dat opravným kódem, který zajistí jejich opravu při výskytu chyb. Samozřejmě je možné výše nastíněné techniky kombinovat a vytvořit tak zabezpečení dle požadavků na výslednou aplikaci.

Dalším možným členěním odolnosti proti poruchám je rozlišování pasivních a aktivních metod. Pasivní metody [4] jsou založeny na předpokladu, že je možné zjistit všechny možné poruchy a pro každou z nich předem nachystat řešení, které snižuje její dopad. U jednoduchých problémů takové omezení nemusí vadit, ale pro rozsáhlé aplikace může být značně náročné analyzovat takové poruchy nebo mít připravené a uložené potřebné opravy a náhrady může být značně prostorově náročné. Ovšem při výskytu poruchy nevzniká zbytečná prodleva do znovuobnovení funkcionality. To je zásadní rozdíl od aktivního přístupu, kdy příslušnou poruchu je třeba analyzovat a následně připravit řešení na míru za běhu. I když odpadá potřeba mít připravené kompenzace napravující poruchu tím, že se počítají za běhu, jejich výpočet zabere určitý výpočetní čas, kdy je zařízení v nedefinovaném stavu. Odstraněním zásadních problémů a kombinací obou přístupů se zabývá hybridní metoda [11], kterou je možné shrnout v následujícím postupu. V aplikaci je detekována porucha. Využije se pasivní přístup, kdy je porucha co nejlépe kompenzována a současně je spuštěna její diagnostika. Po ní je možné připravit opravu na míru. Až je oprava připravena, tak je aplikována pomocí rekonfigurace systému. Tímto způsobem je možné opravit i předem neočekávané poruchy a zároveň je odstraněna doba nedefinované funkce. Jsou tedy využity silné stránky jednotlivých přístupů a současně potlačeny podstatné nedostatky.

Výše zmíněné přístupy lze aplikovat i na programovatelná hradlová pole FPGAs *Field Programmable Gate Arrays* [7], která se stále více uplatňují v nejrůznějších systémech díky svému výpočetnímu výkonu a schopnosti změnit svou konfiguraci pro přizpůsobení se aktuálním podmínkám. Jejich hlavní nevýhodou je náchylnost nejen na kosmické záření, které způsobuje poruchy konfigurační paměti. Dle intenzity a doby působení může způsobit přechodné, ale i trvalé poruchy. Typickou poruchou je překlopení jednoho náhodného bitu libovolné paměti např. té konfigurační. Tato porucha je známa pod označením *Single Event Upset (SEU)*. Odolnost proti poruchám může být zajištěna jejich maskováním pomocí zdvojení s porovnáním *(DwC – Duplication with Comparison)* podle schématu na obrázku 1 nebo pomocí tří-modulové redundance *(TMR – Triple Modular Redundancy)* podle schématu na obrázku 2. V modulech může být obsažen jak celý obvod, tak i jen jeho důležité částí. Dále je také možné využít zřetězení příslušných přístupů a rozdělit tak obvod na menší zabezpečené části.



Obrázek 1. Schéma DwC



Obrázek 2. Schéma TMR

Další možností, která již skutečné provádí opravu poruch, je přístup, kdy je konfigurační informace daného FPGA přepsána pomocí správné konfigurace *(golden bitstream)*. Tento přístup, při kterém dochází k rekonfiguraci FPGA, se nazývá *Scrubbing*. Pro uložení *golden bitstreams* je potřeba mít k dispozici radiačně odolnou paměť. Takový požadavek je možné zajistit využitím speciálního hardware nebo opatřením dat opravným kódem. Jiným přístupem je *Lazy Scrubbing* [3], který využívá násobného výskytu stejných konfigurací v rámci TMR. Když je na FPGA daná část v TMR, pak každý modul je vytvořen díky stejné konfiguraci, která je tudíž uložena v konfigurační paměti FPGA také třikrát. V takovém případě už není potřeba paměť s *golden bitstreams* a v případě poruchy v jednom z těchto modulů, je konfigurační informace příslušného porouchaného modulu přepsána pomocí majoritního výskytu konfiguračních informací z těchto tří stejných modulů. Neboli z konfigurační paměti FPGA jsou přečteny příslušné konfigurační informace všech tří modulů. Dále je pro každý odpovídající si bit určena majoritní hodnota a následně je takto vytvořený bitstream opět nahrán do konfigurační paměti díky částečné rekonfiguraci [9] tzn. možnosti rekonfigurovat jen určitou část FPGA. Obstarat vše potřebné k částečné dynamické rekonfiguraci by měl její řadič, tedy speciální přidaná komponenta.

III. Řadič částečné dynamické rekonfigurace

Pro aktivní přístup k odolnosti proti poruchám je řadič částečné dynamické rekonfigurace přímo nezbytnou součástí, bez které se nelze v systému obejít. Nejjednodušší variantou je řadič, který provádí *Sbrubbing* s předem danou periodou. Preventivně přepisuje konfigurační paměť a tím také opraví případnou poruchu. Je zřejmé, že takový přístup není příliš efektivní, ale zvýší spolehlivost a nezabere příliš velkou plochu na FPGA. Také nebude příliš náročné jej použít, protože lze přidat k libovolnému již vytvořenému systému prakticky bez modifikace tohoto systému. Zásadní vylepšení přineslo IP jádro od Xilinx *Soft Error Mitigation Controller* [10] pro jejich FPGA řady 7. Konfigurační paměť byla opatřena opravným kódem a tudíž je přidána možnost provádět rekonfiguraci jen v případě výskytu poruchy a navíc opravovat jen porouchanou část. Stejně jako u předchozího přístupu není nutné upravovat zabezpečovaný systém. Ovšem vzniká zde prodleva aktivního přístupu, která je způsobena diagnostikou poruchy, tedy počítáním syndromu poruchy opravného kódu a následně určením porouchaného bitu konfigurační paměti. Jinou možností, která již prodlevou s nedefinovaným výstupem systému netrpí, je propojení tří-modulové redundance a řadiče částečné dynamické rekonfigurace [2]. Zabezpečovaný obvod je nutné uzpůsobit do TMR. Což znamená ztrojnásobení komponent a přidání prvků určujících majoritu ze vstupních hodnot. Dále je nutné opatřit tyto prvky také logikou, která je schopná určit také modul s odlišným výstupem (vstupem prvku počítajícím majoritu). Tuto hodnotu je třeba vyvést na další výstup, který je nutné přidat. Tím se samotný prvek určující majoritu značně zesložití, ale je to potřeba, aby řadič rekonfigurace dostal co nejpřesnější informaci o poruše. S touto informací a dobře namapovaným systémem na FPGA je řadič schopen zajistit dynamickou rekonfiguraci jen porouchaného modulu. Současně s opravou zbylé dva moduly TMR pracují dle specifikace a tudíž i celý systém pracuje dle specifikace. Protože prvek určující majoritu bude maskovat výstup jak porouchaného tak i současně opravovaného neboli rekonfigurovaného modulu, jehož výstup nebude po tento čas korektní. Právě takto, jak bylo popsáno, je navržen a implementován *Generic Partial Dynamic Reconfiguration Controller (GPDRC)* [8].

A. Současný stav výzkumu v oblasti řadiče částečné dynamické rekonfigurace

V rámci výzkumné skupiny zabývající se odolností proti poruchám byly postupně navrženy a implementovány dvě verze řadiče částečné dynamické rekonfigurace pro obecné použití na FPGA pod názvem *GPDRC*. První verze [8] je vytvořena tak, aby umožňovala eliminaci přechodných poruch,

jako jsou např. SEU. Pro diagnostiku a přechodné maskování poruch do doby dokončení opravy pomocí rekonfigurace je TMR aplikována na zabezpečovaný systém. V rámci druhé verze řadiče [6] byla původní rozšířena o podporu zotavení systému i z trvalých poruch. Ta je způsobena fyzickým poškozením libovolné části FPGA. Na úrovni tranzistorů dochází k negativní změně jejich vlastností a to např. trvalému zprůchodnění bez ohledu na přiváděné napětí na jejich bázi. U konfigurační paměti to znamená nemožnost změnit stav daného poškozeného uloženého bitu a tedy jeho setrvání v jednom z možných stavů. Důsledkem je nemožnost změnit konfiguraci určité části FPGA, která je ovlivněna právě tímto poškozeným bitem. Pro zotavení se z takové poruchy jsou v FPGA vyhrazeny rezervní bloky. Při odhalení, že se jedná o trvalou poruchu, je příslušný modul vyřazen a nahrazen jinde vyhrazeným náhradním blokem, do kterého je nakonfigurována funkcionalita příslušného vyřazeného modulu. Trvalá porucha je odhalena tak, že i po rekonfiguraci není výstup modulu shodný s ostatními TMR moduly. V případě více se vyskytujících trvalých poruch časem nastane situace, kdy už další rezervní modul není k dispozici. V takovém případě zabezpečení degraduje z TMR na pouhé zdvojení se srovnáním DwC. To už není schopné poruchu lokalizovat přesně, jen ji dokáže oznámit. Následná trvalá porucha způsobí definitivní konec korektní činnosti systému.

B. Budoucí výzkum v oblasti řadiče částečné dynamické rekonfigurace v FPGA

Předchozí výzkum se soustředil na zabezpečení obvodu. Ovšem pokud bude řadič na stejném FPGA jako zabezpečovaný obvod, je velmi pravděpodobné, že může být poruchou zasažen také. V takovém případě není vyloučeno, že řadič s poruchou může způsobit neočekávaným chováním i poškození jinak korektně fungujícího obvodu. Např. by mohl provést rekonfiguraci, která negativně pozmění funkčnost zabezpečovaného obvodu. Proto bude další výzkum směřovat k zabezpečení také samotného řadiče.

I pro řadič rekonfigurace je vhodné využít podobné techniky jako pro zabezpečovaný obvod. A to využít TMR pro maskování poruch jednotlivých modulů s řadiči. Řadič tedy bude v systému třikrát a bude doplněn prvkem určujícím majoritu z jednotlivých výstupů, neboli dat posílaných do konfigurační paměti v rámci rekonfigurace. Tak je vnímána první etapa zabezpečování řadiče. Lze očekávat nepříliš velké zvýšení spolehlivosti, protože řadič zabere trojnásobné místo na FPGA a tudíž se zvýší pravděpodobnost zásahu poruchou. Ovšem oproti tomu bude možná jednonásobná porucha a ve vhodných případech i vícenásobná porucha maskována díky majoritě.

Další etapou zabezpečování bude zavedení rekonfigurace i pro samotné řadiče. Vzhledem ke třem instancím řadiče již se nacházejícím na FPGA by bylo velice vhodné využít právě je. Vize je taková, že předpokládáme poruchu v jednom z modulů ztrojeného řadiče rekonfigurace a tedy v jednom ze tří řadičů v TMR. Tato porucha je rozpoznána díky prvku počítajícímu majoritu a jsou tudíž o ní informovány všechny tyto řadiče. Zbylé dva korektně fungující řadiče se postarají o rekonfiguraci třetího porouchaného. Je vhodné, aby řadič s poruchou do vlastní rekonfigurace nezasahoval. Je nutné zajistit jeho odpojení a tudíž zabránění v činnosti anebo by mělo být postačující využít schopnosti prvku určujícího majoritu, který zajistí maskování chybného výstupu z porouchaného řadiče. I v případě provádění rekonfigurace pouze dvěma funkčními řadiči je možné zjišťovat, zda nenastala porucha. Jedná se o metodu DwC, která ovšem už není schopná určit, ve kterém ze dvou řadičů se porucha projevila. Možným předejitím nastání takové situace je přidat na FPGA ještě jednu instanci řadiče. Celkový počet řadičů by byl čtyři. V případě rekonfigurace jednoho z nich by pořád zbývali tři dobře fungující a tudíž pracující v režimu TMR. I při výskytu další poruchy by ta byla maskována a následně by mohl být nově porouchaný řadič opraven díky opravenému řadiči rekonfigurace a zbylým dvěma korektně fungujícím řadičů. I toto řešení by bylo vhodné otestovat v rámci experimentů.

C. Programová implementace řadiče částečné dynamické rekonfigurace

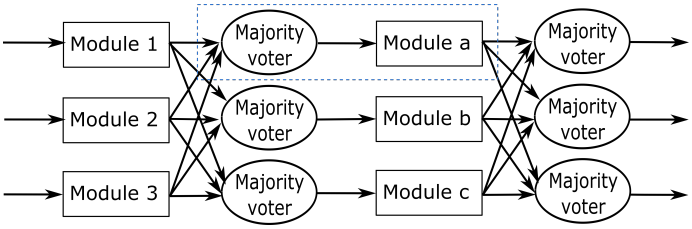
Kromě výše zmíněné implementace GPDRC přímo v hardware se nabízí i alternativa v podobě programové implementace pro procesor. Podstatnou výhodou takového řešení bude odolnost konfigurace proti SEU, pokud tedy nebude procesor implementován v FPGA jako *měkké jádro (soft core)*. V takovém případě by se pro jeho zabezpečení využily stejné techniky, které byly navrženy v předchozím odstavci. Ovšem pokud bude procesor externí součást nebo bude v FPGA v podobě *těžkého jádra (hard core)*, pak mu poruchy konfigurační paměti nehrozí. Jediné, co může SEU způsobit, jsou poruchy v paměťových blocích a tedy chyby v datech potřebných pro činnost. Jedná se o paměť s instrukcemi programu, operační paměť a také registry. Ovšem pro zabezpečení dat proti chybám se nevyužívá rekonfigurace, ale opravné kódy, kterými se data musí opatřit. Lze využít i časové redundance, ale muselo by se zajistit, aby nebylo počítáno opakovaně se stejnými poškozenými daty.

V případě externí součástky jak procesoru tak jiného FPGA s řadičem, je zřejmé, že se prodlouží datové cesty. Tím se prodlouží také čas, který řadič bude potřebovat pro získání informací pro diagnostiku poruchy. Následně bude časově náročnější i samotná rekonfigurace, která bude z poruchy obvod zotavovat. To vše povede k většímu zpoždění opravy a snížení rychlosti výpočtu samotného obvodu. Ovšem záleží na požadavcích na výsledný systém, protože se ušetří plocha na FPGA a také by mohl být procesor využit i k jiné činnosti než pouze pro řadič, když by měl dostatečný výpočetní výkon.

IV. Zabezpečení prvků určujících majoritu

Posledním slabým místem z hlediska spolehlivosti zůstávají prvky určující majoritu u TMR. Ty nejsou nijak zabezpečeny a tudíž při poruše mohou na svém výstupu mít předem neočekávanou hodnotu. Tím mohou způsobit nedefinované chování celého systému. Sice je jejich velikost prakticky zanedbatelná oproti výpočetnímu obvodu, ale i tak při dlouhé době životnosti obvodu šance, že je porucha zasáhne, roste.

Možné zabezpečení je představeno v [1], kde i tyto prvky jsou ztrojeny, což je znázorněno na obrázku 3. Modrou přerušovanou čarou je znázorněn blok, který je třeba rekonfigurovat v případě zjištění poruchy. Oproti původní variantě je v něm zahrnut i jeden prvek určující majoritu. Je to dáno tím, že nelze rozlišit, jestli je porucha v prvku určujícím majoritu anebo v následném modulu. Vše je totiž diagnostikováno až v následující vrstvě prvků určujících majoritu.



Obrázek 3. Schéma TMR se zabezpečenými prvky volícími majoritu

Nelze takto ale zabezpečit poslední instanci po zřetězení, protože je na výstupu potřeba pouze jedna správná hodnota. V tomto případě je výstup ztrojen díky ztrojení prvků počítajících majoritu. Nezbývá než toto poslední zabezpečení omezit a nasadit pouze hlídací obvod popřípadě využít metodu DwC. Při zjištění poruchy je ale nutné výpočet obvodu přerušit do doby, než se pomocí rekonfigurace příslušných zabezpečujících prvků znovu neobnoví korektní funkcionalita. Stejný problém je i u hlídání výstupů z řadičů rekonfigurace v TMR, kdy je opět potřeba jen jeden výstup pro zápis do konfigurační paměti FPGA.

V. Cíle disertační práce

V rámci disertační práce se zaměřuji na vypracování metodiky pro použití řadiče částeční dynamické rekonfigurace pro systémy odolné proti poruchám. Především budu navrhovat a experimentovat s různými kritérii pro návrh, implementaci a samotné používání řadiče. Zatím známá kritéria jsou spolehlivost, rychlost a zpoždění, spotřeba, zabraná plocha na FPGA. Další mohou být identifikována v průběhu výzkumu. Je zřejmé, že jsou vzájemně protichůdná a tak předpokládám vznik různý paretooptimálních řešení, která budou v rámci metodiky diskutována. Zejména jejich přínos pro různé požadavky aplikací.

Vycházím z již vytvořené instance GPDRC, která je výsledkem předchozí práce výzkumné skupiny. Tento řadič budu zabezpečovat pomocí výše nastíněných principů. Dále pro porovnání počítám také s vytvořením implementace pro procesor a variantou s řadičem mimo FPGA s aplikací. Všechny tyto přístupy budou podrobeny experimentům a budou diskutovány přínosy a úskalí, které budou potřeba pro vypracování metodiky.

VI. Závěr

V rámci tohoto článku byly diskutovány základní principy pro odolnost proti poruchám se zaměřením především na FPGA. Obzvláště bylo pojednáváno o prostorové redundanci zajištěné pomocí principu TMR. Ten byl dále rozšířen o možnost částeční dynamické rekonfigurace s využitím přidané diagnostiky do TMR. Tím je možné identifikovat modul TMR, který se má rekonfigurací opravit. Tato rekonfigurace nenaruší činnost obvodu, protože zbylé dva moduly fungují korektně. Vše potřebné k rekonfiguraci musí zajisti její řadič, jehož příkladem je GPDRC vyvinutý v rámci výzkumné skupiny. Ten bude v rámci budoucí práce zabezpečen pomocí zde představených principů. Také bude vytvořena implementace pro procesor, která bude sloužit k porovnání. Vše vede k disertační práci, ve které bude zpracována metodika pro použití řadiče rekonfigurace pro systémy odolné proti poruchám. Zejména půjde o vypracování kriterií pro porovnání jednotlivých přístupů a provedení experimentů, které ukáží, jaký přístup bude pro splnění daných požadavků nejvhodnější.

Poděkování

Tato práce byla podporována Ministerstvem školství, mládeže a tělovýchovy z Národního programu udržitelnosti (NPU II); projektu IT4Innovations excellence in science – LQ1602. Tato činnost byla rovněž podporována projekty řešenými na VUT v Brně pod číslem FIT-S-14-2297.

Reference

[1] Abraham, J. A.; Siewiorek, D. P.: An Algorithm for the Accurate Reliability Evaluation of Triple Modular Redundancy Networls. *IEEE Transactions on Computers*, ročník c-23, č. 7, červenec 1974: s. 682–692.

[2] Bolchini, C.; Miele, A.; Santambrogio, M. D.: TMR and Partial Dynamic Reconfiguration to mitigate SEU faults in FPGAs. *22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems (DFT 2007)*, září 2007, ISSN 1550-5774, s. 87–95, doi:10.1109/DFT.2007.25.

[3] Garvie, M.: *Reliable Electronics through Artificial Evolution*. Disertační práce, University of Sussex, leden 2005.

[4] Jiang, J.; Yu, X.: Fault-tolerant control systems: A comparative study between active and passive approaches. *Annual Reviews in Control*, ročník 36, č. 1, 2012: s. 60–72, ISSN 1367-5788, doi: http://dx.doi.org/10.1016/j.arcontrol.2012.03.005.

[5] Koren, I.; Krishna, C. M.: *Fault-Tolerant Systems*. Elsevier, 2007, ISBN 9780120885251.

[6] Miculka, L.; Kotasek, Z.: Generic partial dynamic reconfiguration controller for transient and permanent fault mitigation in fault tolerant systems implemented into FPGA. *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, duben 2014, s. 171–174, doi:10.1109/DDECS.2014.6868784.

[7] Siegle, F.; Vladimirova, T.; Ilstad, J.; aj.: Mitigation of Radiation Effects in SRAM-Based FPGAs for Space Applications. *ACM Comput. Surv.*, ročník 47, č. 2, leden 2015: s. 37:1–37:34, ISSN 0360-0300, doi: 10.1145/2671181.
URL http://doi.acm.org/10.1145/2671181

[8] Straka, M.; Kastil, J.; Kotasek, Z.: Generic partial dynamic reconfiguration controller for fault tolerant designs based on FPGA. *NORCHIP 2010*, listopad 2010, s. 1–4, doi:10.1109/NORCHIP.2010.5669477.

[9] XILINX: Partial Reconfiguration User Guide. Dostupné z: http://www.xilinx.com/support/documentation/sw_manuals/xilinx14_1/ug702.pdf, duben 2012 [cit. 2017-06-07].

[10] XILINX: Soft Error Mitigation Controller v4.1. Dostupné z: https://www.xilinx.com/support/documentation/ip_documentation/sem/v4_1/pg036_sem.pdf, duben 2017 [cit. 2017-06-12].

[11] Yu, X.; Jiang, J.: Hybrid Fault-Tolerant Flight Control System Design Against Partial Actuator Failures. *IEEE Transactions on Control Systems Technology*, ročník 20, č. 4, červenec 2012: s. 871–886, ISSN 1063-6536, doi:10.1109/TCST.2011.2159606.